

CLAIMS

What is claimed is:

- 5 1 A method for facilitating file access in a peer-to-peer network, the peer-to-peer network including a plurality of nodes, wherein a portion of the nodes are separated from the network by a firewall device, the method comprising the steps of:
- (a) designating a first node that is not firewall protected to act as a proxy server;
- (b) in response to determining that a second node is protected by a firewall, instructing the second node to establish a connection with the proxy server;
- (c) sending an open connection request from the second node to the proxy server;
- (d) in response to receiving a request from a third node for a file on the second node, instructing the third node to send the request to the proxy server; and
- (e) forwarding the request from the proxy server to the second node as a response to the open connection request, thereby allowing other nodes to access files on the second node despite the presence of the firewall.
- 20

2 The method of claim 1 further including step of:

- (f) sending a response from the second node to the proxy server, and forwarding the response from the proxy server to the third node, wherein the response includes the requested file.

5

3 The method of claim 2 wherein step (b) further includes the steps of:

- (i) allowing the second node to report its IP address,
- (ii) sending a probe message to the second node,
- (iii) observing what IP address the second node is connecting from,
- (iv) comparing the observed IP address with the reported IP address, and
- (v) determining that the second node is protected by the firewall when the IP addresses mismatch.

10

15

4 The method of claim 3 wherein step (b) further includes the step of:

- (i) allowing the proxy server to report its IP address,
- (ii) sending a probe message to the proxy server,
- (iii) observing what IP address the proxy server is connecting from,
- (iv) comparing the observed IP address with the reported IP address, and
- (v) determining that the proxy server is not protected by a firewall when the IP addresses match.

20

5 The method of claim 1 wherein step (c) further includes the step of sending a message from the proxy server to a node registry that registers the second node using the IP address of the proxy server.

5 6 The method of claim 5 wherein step (d) further includes the step of in response to receiving a search request from the third node for a file, returning a result to the third node, wherein the result identifies a file name, the second node, and the IP address of the proxy server.

10 7 The method of claim 6 wherein step (d) further includes the step of sending a request to the proxy server using the IP address of the proxy server, wherein the request includes a URL for the file on the second node.

15 8 The method of claim 6 wherein step (d) further includes the steps of receiving the request by the proxy server, and determining if the request is intended for the proxy server or the second node by examining the URL in the request.

20 9 The method of claim 6 wherein step (d) further includes the step of a response to determining that the request is intended for the second client node, reformatting the request so that the second node may respond to the request.

10 A peer-to-peer file delivery network including a plurality of nodes, wherein a portion of the nodes are separated from the network by a firewall device, the network comprising the steps of:

means for designating a first node that is not firewall protected to act as a proxy server;

means for instructing a second node to establish a connection with the proxy server in response to determining that the second node is protected by a firewall;

means for sending an open connection request from the second node to the proxy server;

means for instructing a third node to send a request to the proxy server in response to receiving the request from the third node for a file on the second node; and

means for forwarding the request from the proxy server to the second node as a response to the open connection request, thereby allowing other nodes to access files on the second node despite the presence of the firewall.

11 The network of claim 10 wherein a response that includes the requested file is sent from the second node back to the proxy server, and forwarded from the proxy server to the third node.

12 The network of claim 11 wherein the means for instructing the second node
to establish a connection with the proxy server further includes:

means for allowing the second node to report its IP address,

means for sending a probe message to the second node,

means for observing what IP address the second node is connecting
from,

means for comparing the observed IP address with the reported IP
address, and

means for determining that the second node is protected by the
firewall when the IP addresses mismatch.

13 The network of claim 12 wherein the means for instructing the second node
to establish a connection with the proxy server further includes:

means for allowing the proxy server to report its IP address,

means for sending a probe message to the proxy server,

means for observing what IP address the proxy server is connecting
from,

means for comparing the observed IP address with the reported IP
address, and

means for determining that the proxy server is not protected by a
firewall when the IP addresses match.

14 The network of claim 10 further including a node registry for receiving a message from the proxy server to register the second client node using the IP address of the proxy server.

5 15 The network of claim 10 wherein the means for instructing the third node further includes:

means responsive to receiving a search request from the third node for the file, for returning a result to the third node, wherein the result identifies a file name, the second node, and the IP address of the proxy server.

10 16 The network of claim 15 wherein the means for instructing the third node further includes means for sending a request to the proxy server using the IP address of the proxy server, wherein the request includes a URL for the file on the second node.

15 17 The network of claim 15 wherein the means for instructing the third node further includes means for receiving the request by the proxy server, and determining if the request is intended for the proxy server or the second node by examining the URL in the request.

20 18 The network of claim 15 wherein the means for instructing the third node further includes means for a response to determining that the request is

intended for the second client node, reformatting the request so that the second node may respond to the request.

5 19 A method for facilitating file access in a peer-to-peer network, the peer-to-peer network including a plurality of nodes, wherein at least one of the nodes is protected from the network by a firewall device, the method comprising the steps of:

- 10 (a) instructing the firewall-protected client node to transmit a first request a first node on the network in order to establish an open connection with the first node;
- (b) instructing other nodes in the network to send requests for files on the firewall-protected client to the first node;
- (c) receiving a request on the first node for a file on the firewall-protected client from a second node;
- 15 (d) passing the request for the file over the open connection to the firewall-protected client as a response to the first request;
- (e) responding to the request for the file by sending a response, which includes the file from the firewall-protected client to the first node; and
- 20 (f) passing the response from the first node to the second node, wherein the first node acts as a proxy between the firewall-protected node and the second node to allow the second node to access the file on the firewall-protected node.

20 The method as in claim 19 further including the step of waiting to respond to the first request until receiving a request intended for firewall-protected client.

21 The method as in claim 20 further including the step of: upon termination of the connection, instructing the firewall-protected client to reestablish communication with the first node.

5

09779344-043404
TOP SECRET